In the Claims

Please amend the claims as follows:

1. (Previously Presented) Method for authenticating a third tier server system in a distributed application environment, wherein said distributed application environment comprising client system having parts of the distributed application, server systems having the remaining parts of the distributed application, and third tier server system which exchanges data between said client system and said server systems, wherein said client system acts as single point of recognizing and managing third tier server certificates and provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment, wherein at said server systems side said method comprises:

receiving from said common database of said client system at least all necessary information of a third tier server certificate being accepted as trustworthy for determining to accept or to decline a connection to said third tier server,

comparing said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system,

accepting said third tier server system as to be authenticated if said at least all necessary information matches said server-copy of the third tier certificate.

2. (Previously Presented) Method according to claim 1, wherein said at least all necessary information from said client system is received via a non-continuous client-server connection.

3. (Original) Method according to claim 2, wherein said non-continuous client-server connection is using a secure transmission protocol.

4. (Previously Presented) Method according to claim 1, wherein said at least all necessary information consists essentially of a client-copy of said third tier server certificate as stored in the common data base of said distributed application environment, and a server name which has transmitted said client-copy of said third tier server certificate to said client system.

5. (Previously Presented) Method according to claim 1, wherein said at least all necessary information consists essentially of a fingerprint of a client-copy of said third tier certificate, and a server name which has transmitted said client-copy of said third tier server certificate to said client system.

6. (Previously Presented) Method according to claim 1, wherein said at least all necessary information consists essentially of two different fingerprints of a client-copy of the third tier server certificate, a server name which has transmitted said client-copy of the third original tier server certificate to said client system, and a certificate name.

7. (Previously Presented) Method for authenticating a third tier server system in a distributed application environment, wherein said distributed application environment comprising a client system having parts of the distributed application, server systems having the remaining parts of the distributed application, and a third tier server system which exchanges data between said client system and said server systems, wherein said client system provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment, wherein at said client system said method comprises:

receiving a client-copy of a third tier server certificate from a third tier server system,

determining whether said received client-copy of said third tier server certificate can be accepted as trustworthy,

storing said client-copy of said third tier server certificate in said common data base of the distributed application environment if said client-copy of said third tier server certificate has been accepted as trustworthy, and

transferring to each server of said server systems at least all necessary information of said client-copy of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server system.

8. (Previously Presented) Method according to claim 7, wherein said storing ~~step~~ additionally includes storing a name of said third tier server system that has transmitted said client-copy of said third tier certificate.

9. (Previously Presented) Method according to claim 7, wherein said client-copy of said third tier server certificate is received via a secure transmission protocol.

10. (Previously Presented) Method according to claim 7, wherein said at least all necessary information is transmitted to said each server of said server systems via a non-continuous secure connection.

11. (Original) Method according to claim 8, wherein authentication of said client system is accomplished by user ID and/or password.

12. (Previously Presented) System for authenticating a third tier server system in a distributed application environment, wherein said distributed application environment comprises a client system having parts of the distributed application,-and application server systems having the remaining parts of the distributed application, wherein said application server systems-comprise:

a transfer server component which, in a first computer process, supports non-continuous and secure client-server connection for receiving certificate information from a client of a third tier server certificates being accepted as trustworthy for determining to accept or to decline a connection to said third tier server system,

a connection negotiator component which, in a second computer process receives incoming third tier server certificates via a secure connection between said application server systems and said third tier server,

a certificate verifier component which, in a third computer process, compares said third tier server certificate received from said third tier server with said certificate information received from said client.

13. (Previously Presented) System according to claim 12, wherein said certificate information comprises two different fingerprints of the original third tier server certificate, name of the server which has transmitted said third tier server certificate to said client system, and certificate name.

14. (Previously Presented) System according to claim 13, wherein said two different fingerprints are generated by applying two different algorithms to said third tier server certificates received from said common database.

15. (Previously Presented) System according to claim 14, wherein said application server systems further include the same algorithms as used for generating said two different fingerprints.

16. (Previously Presented) Client system for authenticating third tier server in a distributed application environment, said distributed application environment comprises a client system having parts of the distributed application, application server systems having the remaining parts of the distributed application, said client system comprising:

a connection negotiator component which, in a first computer process, receives incoming third tier server certificate via a secure connection from said third tier server,

a common data base of the distributed application environment which, in a second computer process, stores said third tier server certificates received from said third tier server system which have been accepted as trustworthy for the distributed application environment,

a certificate verifier component which, in a third computer process, compares said received third tier server certificate with information stored in said common database and stores them into said common database if it matches,

a user interface component which, in a fourth computer process, allows for accepting or rejecting an unknown third tier server certificate not contained in said common data base, and

a certificate transmitter component which, in a fifth computer process, generates certificate information of said third tier server certificates being accepted as trustworthy

for determining to accept or to decline a third tier server from said common database and transmits them to said application server systems via a secure connection.

17. (Previously Presented) Computer program product stored in the internal memory of a computer, containing parts of software code to execute the method in accordance with claim 1 if the product is run on the computer.

18. (Previously Presented) System according to claim 15, further comprising a client system comprising:

a connection negotiator component for receiving incoming third tier server certificates via a secure connection from said third tier server,

a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment,

a certificate verifier component for comparing received third tier server certificate with information stored in said common database and storing them into said common database if it matches,

a user interface component allowing to reject or accept an unknown third tier server certificate not contained in said common data store, and

a certificate transmitter component for extracting all necessary information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database and transmitting them to said server systems via a secure connection.

19. (Previously Presented) System according to claim 16, further comprising an application server system comprising:

a transfer server component supporting non-continuous and secure client-server connection,

a connection negotiator component for receiving incoming third tier server certificate via a secure connection between said server systems and said third tier server,

a certificate verifier component for comparing said third tier server certificate received from said third tier server with said information received from said client system for determining to accept or to reject third tier server, and

a third tier server which exchanges data between said client system and said server.